A Finite Field or a Vector Space ?

Gohar Kyureghyan

Otto-von-Guericke University, Magdeburg, Germany

A variety of problems on optimal or extremal objects in Combinatorics, Coding Theory, Cryptology and Finite Geometry can be reduced to characterization or construction of mappings of finite fields with specific properties.

Let $\mathbb{F}_q$ be the finite field with q elements. Any mapping of $\mathbb{F}_q$ into itself is given by a univariable polynomial over $\mathbb{F}_q$ of degree less than q. If $q = s^n$, with $n \geq 1$, then $\mathbb{F}_q$ is an n-dimensional vector space over its subfield $\mathbb{F}_s$. Let $(x_1, \ldots, x_n)$ be the coordinate vector of $x \in \mathbb{F}_q$ with respect to a fixed basis $\mathcal{B}$ of $\mathbb{F}_q$ over $\mathbb{F}_s$. Then any polynomial $F(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$ defines a mapping of $\mathbb{F}_q$ via $(x_1, \ldots, x_n) \mapsto F(x_1, \ldots, x_n)$. Moreover, any mapping F on $\mathbb{F}_q$ can be represented by a unique polynomial $F(X_1, \ldots, X_n) \in \mathbb{F}_q[X_1, \ldots, X_n]$ of degree less than s in every variable X_i. Note that the multivariate representation of F is basis dependent.

In this talk, we present several problems on mappings of finite fields. We show that in certain cases it is more convenient to consider mappings on finite fields as those of vector spaces and vice versa.